

Applicant: Satyendra Yadav  
Serial No.: 10/066,070  
Filed: February 1, 2002

Attorney's Docket No.: 10559-754001/P13652

### REMARKS

Claims 1-30 are pending in this application, with claims 1, 12, 21 and 29 being independent. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-30 stand rejected under 35 U.S.C. 102(b) as allegedly being unpatentable over Trostle (US 5,919,257). This contention is respectfully traversed.

Trostle describes examining executable programs during pre-boot of a workstation to determine if any illicit changes have been made to the selected executable programs; and if changes are detected, the user and/or administrator is notified. (See Trostle at col. 1, line 66 to col. 3, line 3.) This is clearly different than "examining a set of instructions embodying an invoked application to identify the invoked application", as recited in independent claim 1. First, the executable programs of Trostle are deliberately examined during pre-boot, which is before the applications are invoked.

Second, Trostle describes hashing multiple executable programs at once to calculate a single hash value. (See Trostle at col. 2, lines 61-67.) This hashing approach cannot be used to identify a specific application and is not intended for such. Trostle does mention an alternative embodiment in which a hash

Applicant: Satyendra Yadav  
Serial No.: 10/066,070  
Filed: February 1, 2002

Attorney's Docket No.: 10559-754001/P13652

value may be computed for each individual executable program (col. 3, lines 3-7), but this is done to determine which of the selected executable programs has been corrupted (col. 7, lines 25-27), not to identify an invoked application. The difference here is made clear by Trostle's description of the selection process, in which "some randomness" is used "with a goal of checking all the workstation executable programs within a reasonable number of workstation resets." (See Trostle at col. 3, lines 8-18.)

In addition, independent claim 1 recites, "examining a set of instructions embodying an invoked application to identify the invoked application; obtaining an application-specific intrusion detection signature; and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion." (Emphasis added.) The present specification defines "intrusion" as "an attempt to break into and/or misuse a computing system", and defines "intrusion signature" as "a communication pattern identified as corresponding to a known type of intrusion, including patterns that may be found in individual packets and patterns that may be gleaned from analyzing multiple packets." (See Specification at ¶ 18.)

Applicant: Satyendra Yadav  
Serial No.: 10/066,070  
Filed: February 1, 2002

Attorney's Docket No.: 10559-754001/P13652

The cited portions of Trostle (col. 5, lines 28-42; and col. 6, lines 13-17) describe the use of signed pre-boot modules to enhance security between workstation and server, and a signature "used for background authentication and to further assist in validating the authenticity of packets transmitted by the workstation onto the network." The "signatures" being described here are clearly referring to digital signature techniques (e.g., encrypting a pre-boot module with a private key of a private-public key pair). (See Trostle at col. 5, lines 32-46.) This is completely different than the claimed obtaining an application-specific intrusion detection signature, and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion. Trostle does not describe monitoring network communications as claimed; Trostle's focus is pre-boot detection of prior illicit changes to executable programs, not network packet filtering.

In view of this clarification of the teachings of Trostle, each of independent claims 1, 12, 21 and 29 should be in condition for allowance. Furthermore, dependent claims 2-11, 13-20, 22-29, and 30 should be patentable based on the above arguments and the additional recitations they contain.

Applicant: Satyendra Yadav  
Serial No.: 10/066,070  
Filed: February 1, 2002

Attorney's Docket No.: 10559-754001/P13652

For example, with respect to claims 2, 13, and 30, the cited portion of Trostle (col. 3, lines 19-30) describes how the hash function and the trusted hash value can be downloaded during pre-boot in a manner that is transparent to the user and provides a trusted technique for detecting illicit changes to executable programs. Trostle does not describe tracking one or more characteristics of network communications to identify process-specific abnormal communication behavior. Thus, claims 2, 13, and 30 should be in condition for allowance for at least these additional reasons.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art

Applicant: Satyendra Yadav  
Serial No.: 10/066,070  
Filed: February 1, 2002

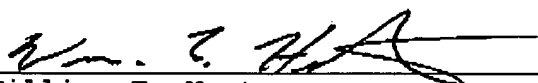
Attorney's Docket No.: 10559-754001/P13652

teaches or suggests the features which are claimed, and  
therefore that all of these claims should be in condition for  
allowance. A formal notice of allowance is thus respectfully  
requested.

Please apply any necessary charges or credits to Deposit  
Account No. 06-1050.

Respectfully submitted,

Date: October 26, 2005

  
\_\_\_\_\_  
William E. Hunter  
Reg. No. 47,671

Fish & Richardson P.C.  
12390 El Camino Real  
San Diego, California 92130  
Telephone: (858) 678-5070  
Facsimile: (858) 678-5099

10556962.doc